WHITEPAPER

Security Operation Center: *Make Or Buy?*

sure[secure]

1. Wofür brauche ich ein Security Operation Center eigentlich?

Ein Security Operation Center (SOC) ist eine Organisationseinheit und bildet die zentrale Leitstelle für Security-Events. Das SOC hat die Aufgabe das Unternehmen zu schützen und umfasst die Überwachung, Erkennung und Reaktion auf Cybersecurity-Bedrohungen. Ein SOC ist vor allem deshalb spannend, weil es in der Lage ist verschiedenste Log-Quellen aufzugreifen und diese Daten zu korrelieren. Das Credo ist: Turn data into doing.

Das Security Operation Center verfügt über 5 Kernfunktionen:

1. **Frühzeitige Erkennung und Abwehr von Bedrohungen:**
   Durch die Kombination aus marktführenden Technologien, Tools, Prozessen und Experten-Teams können Systeme, Netzwerke und Anwendungen auf Anzeichen bösartiger Aktivitäten geprüft werden.

2. **Reaktion auf Sicherheitsvorfälle:**
   Wird ein Sicherheitsvorfall identifiziert, ist das SOC die erste Instanz, die diesen erkennt und ist direkt verantwortlich für die Koordinierung von Erstmaßnahmen. Dies ist in der Regel die Eindämmung, um weitere Infrastruktur-Bestandteile zu schützen.

3. **Compliance:**
   Das SOC leistet einen essenziellen Beitrag zur Einhaltung von Datenschutzvorschriften und Compliance-Standards.

4. **Sicherheitsstrategie und -verbesserung:**
   Durch das Sammeln vielfältiger Log-Quellen und Anomalien, kann die Security-Strategie sukzessive verfeinert werden, um die Cyber-Resilienz zu steigern.

5. **Krisen-Resilienz:**
   Durch die frühzeitige Erkennung von Cyberangriffen und Anomalien, können die kostspielige Ereignisse wie Datenverletzungen oder Ausfallzeiten verhindert werden. Zusätzlich stellt ein SOC sicher, dass kritische Systeme nicht ausfallen. Dadurch bleibt die Geschäftskontinuität gewährleistet.

2. Wie ist ein Security Operation Center aufgebaut?

Ein typisches SOC besteht jedoch aus drei Schlüsselelementen.

Das sind:
- **People (Experten-Teams)**
- **Products (Technologien)**
- **Processes (Klare Strukturen und Abläufe)**

People:

Ein SOC funktioniert nur dann gut, wenn interdisziplinäre Teams zusammenkommen. Ein Team aus reinen Security-Analysten ist nicht zielführend, da wichtige Kompetenzen fehlen. Folgende Spezialisierungen sollten in jedem Security Operation Center vorhanden sein:

- **Analysten:**
  Sicherheitsanalysten sind die Fachleute an vorderster Front, die nach der Automatisierung Anomalien prüfen und bearbeiten. Sie spielen eine entscheidende Rolle bei der Erkennung, Einordnung und Eindämmung von Sicherheitsbedrohungen.

- **Vorfallsreaktionsteam:**
  Ein gut definiertes Incident Response Team ist ein wesentlicher Bestandteil der SOC-Struktur. Dieses Team ist für die Koordinierung und Ausführung von Notfallplänen bei Sicherheitsvorfällen verantwortlich. Dazu gehört vor allem auch mindesten ein dedizierter Incident Manager.

- **Security DeVops:**
  Die eingesetzten Technologien bieten in der Regel die Möglichkeit zur Entwicklung von eigenen Detections. Diese zu bauen ist nicht trivial und benötigt eine spezielle Ausbildung. Für eine optimale SOC-Konfiguration ist diese Kompetenz unerlässlich.

- **Forensiker:**
  Diese Spezialisten suchen proaktiv nach versteckten oder fortgeschrittenen Bedrohungen, die möglicherweise keine Standard-Sicherheitswarnungen auslösen. Sie verwenden Datenanalysen und spezielle Tools, um potenzielle Sicherheitsprobleme zu identifizieren.

- **Management:**
  Das SOC wird in der Regel von einem Manager geleitet, der den täglichen Betrieb überwacht, sich mit anderen Abteilungen abstimmt, Richtlinien und Verfahren festlegt und sicherstellt, dass das SOC mit der Sicherheitsstrategie des Unternehmens übereinstimmt.

Products:

Ein SOC stützt sich auf eine breite Palette von Sicherheitstools und -technologien, essenziell sind die folgenden:

- **Sicherheitsinformations- und Ereignisverwaltungssysteme (SIEM):**
  Die Schlüsseltechnologie für jedes Security Operation Center. Diese Tools sammeln und analysieren Protokolle und Ereignisse aus verschiedensten Log-Quellen. Sowohl Cloud- als auch On-Premise Quellen können angebunden werden, um Datenströme nutzbar zu machen. So schafft es ein SIEM Anomalien schnell visible und nachvollziehbar zu machen. Diese Tools verfügen in der Regel auch über Anbindungen zu Bedrohungsinformations-Plattformen, sodass aktuelle Bedrohungsmuster schnell identifiziert werden können.

- **Schwachstellen-Scanner:**
  Diese Tools helfen bei der Ermittlung und Bewertung von Schwachstellen in den Systemen und Anwendungen des Unternehmens.

- **SOAR-Plattformen (Security Orchestration, Automation, and Response):**
  Diese Plattformen automatisieren Aufgaben zur Reaktion auf Vorfälle und tragen zur Verbesserung der SOC-Effizienz bei. Damit dies gut funktioniert, ist die Konfiguration entscheidend.

- **Forensik und Packet Capture Tools:**
  Diese Tools werden für die Untersuchung von Sicherheitsvorfällen und die Analyse des Netzwerkverkehrs eingesetzt wie z. B. SIGMA, Yara, SIFT, Autopsy uvw.

Processes:

Best-Practices, Vorschriften und Sicherheitsrichtlinien sind in den Prozessen eines SOCs fest verankert. Klare Abläufe sind definiert, um Vorfälle schnell und sauber zu behandeln. Darüber hinaus sind auch Kommunikations- und Eskalationsprozesse ausdefiniert, wenn es um die Zusammenarbeit mit Externen oder anderen Abteilungen geht. Diese Prozesse stellen sicher, dass kritische Vorfälle bei Bedarf an höhere Managementebenen weitergeleitet werden. In der Regel verfügen SOCs über eine Tier3-Struktur.

Weitere Prozesse für Schulungs- und Weiterbildungsprogramme, sowie für das Reporting und die Dokumentation runden den Block ab.
##24/7

3. Was kann ich von einem SOC erwarten und was nicht?

Das können Sie erwarten	Das können Sie nicht erwarten
Frühzeitige Erkennung von Bedrohungen durch Echtzeitüberwachung und -analyse von Sicherheitsereignissen	Sofortige Beseitigung von Bedrohungen
24x7 Überwachung, um eine kontinuierliche Sicherheitsüberwachung zu gewährleisten und das Risiko unentdeckter Bedrohungen zu verringern	Keine Sicherheitsvorfälle mehr. Diese können dennoch auftreten; die Hauptaufgabe eines SOC besteht darin, ihre Auswirkungen zu minimieren (zB durch frühzeitige Erkennung)
Sicherheitswarnungen über potenzielle Bedrohungen und Vorfälle	Null Fehlalarme: Da gerade zu Beginn kein System perfekt ist, kann es zu Fehlalarmen oder -warnungen kommen.
Unterstützung bei der Einhaltung gesetzlicher Vorschriften und Compliance-Anforderungen.	Lösung von nicht sicherheitsrelevanten Problemen: Ein SOC konzentriert sich auf die Sicherheit.
Schutz sensibler Daten vor Cyber-Bedrohungen.	Einmal-Investition: Die Aufrechterhaltung eines SOC ist mit Kosten für Personal, Technologie und Schulung verbunden.
Daten zur Verfeinerung von Sicherheitsstrategien und zur Verbesserung des Schutzes im Laufe der Zeit.	

4. Die Gretchen-Frage: Make or Buy?

Bei der Make-or-Buy Entscheidung gibt es neben dem Budget noch weitere, wichtige Aspekte. Möchte ich ein SOC selber hochziehen, obliegt es auch mir die drei wesentlichen Bausteine – Products, People, Process – vorzuhalten und auszudefinieren. Das versetzt mich in die Lage die volle Kontrolle, aber auch die volle Verantwortung zu tragen. Das gilt auch für die eventuell zu beschaffende Infrastrukturen – je nach Betriebsmodell. Das wiederum kann vor allem den Projektstart zeitlich aufwändiger gestalten als eigentlich nötig.

Make	Buy
Anpassung: Die Erstellung eines SOC ermöglicht die Anpassung an die spezifischen Bedürfnisse und Anforderungen Ihres Unternehmens und gewährleistet einen individuelleren Sicherheitsansatz.	Kosteneffizienz: Das Outsourcing eines SOC kann kosteneffizienter sein, da es die Vorlaufkosten für den Aufbau und die Wartung eines SOC reduziert.
Volle Kontrolle: Sie haben die vollständige Kontrolle über die Gestaltung des SOC, die Personalausstattung und die Wahl der Technologie.	Spezialisiertes Wissen: SOC-Dienstleister verfügen oft über spezielles Fachwissen und haben Zugang zu den neuesten Technologien und Bedrohungsdaten.
Eigenes Fachwissen: Sie können internes Fachwissen und Fähigkeiten entwickeln und so ein tieferes Verständnis für Ihre Sicherheitsumgebung entwickeln.	Schnelle Bereitstellung: Der Kauf eines SOC kann zu einer schnelleren Implementierung und einer schnelleren Reaktion auf neue Bedrohungen führen.
24x7	Skalierbarkeit: Viele SOC-Dienstleister bieten skalierbare Lösungen an, die sich an die sich entwickelnden Anforderungen Ihres Unternehmens anpassen lassen.
	24x7

Die Entscheidung hängt von der Größe, dem Budget, dem vorhandenen Fachwissen und den Sicherheitsprioritäten Ihres Unternehmens ab. Einige entscheiden sich für den Aufbau eines SOC, um die volle Kontrolle zu haben, während andere aus Kostengründen und wegen des Zugangs zu externem Fachwissen einen SOC-Service kaufen. Es ist auch möglich, beide Ansätze zu kombinieren, indem man ein internes SOC aufbaut und es durch ausgelagerte Dienste ergänzt. Letztlich hängt die richtige Wahl von Ihren individuellen Umständen und Zielen ab.

5. Woran scheitern die meisten SOC-Projekte?

Immer wieder gibt es SOC-Projekte, die an irgendeiner Stelle scheitern. Die Gründe dafür können unterschiedlich sein. Häufig sind die Gründe dafür in einer unsauberen Vorbereitung zu finden. Wurde z. B. bei der Budgetplanung in der Make-Decision der Punkt Personal ausreichend beleuchtet? Oder war klar, welche Ziele mit dem SOC-Projekt erreicht werden sollten? Ohne klare Zielstellungen, ist es schwierig den Erfolg auszuweisen.
Essenziell sind auch die Überlegungen in Richtung Prozesse. Diese sollten nicht erst diskutiert werden, wenn Personal und Produkte schon ausgearbeitet sind. Hier gibt es Abhängigkeiten in beide Richtungen.

Ein klares und durchdachtes Konzept ist die Basis für das Gelingen. Das gilt auch für die Buy-Decision. Auch hier sollte im Vorfeld klar sein, was die Zielstellung ist.

6. Möglichkeiten und Betriebsmodelle, wie sieht das SOC der Zukunft aus?

- **Eigenes SOC:**
  Das SOC wird intern von der Organisation aufgebaut und betrieben. Dieses Modell bietet maximale Kontrolle und Anpassungsfähigkeit, erfordert jedoch erhebliche Investitionen in Personal, Technologie und Schulungen. Es wird oft von großen Unternehmen und Organisationen mit spezifischen Sicherheitsanforderungen bevorzugt.

- **Hybrides SOC:**
  Dieses Modell kombiniert interne und externe Ressourcen. Die Organisation betreibt ein internes SOC und ergänzt es bei Bedarf durch externe Dienstleister oder Managed Security Service Providers (MSSPs). Es bietet Flexibilität und Skalierbarkeit.

- **MSSP oder Outsourcing:**
  Die Organisation beauftragt einen Drittanbieter (MSSP) mit der Bereitstellung von SOC-Diensten. Dieses Modell kann kostengünstiger sein und ermöglicht einen schnelleren Start, erfordert jedoch eine gute externe Zusammenarbeit und das Teilen von Sicherheitsdaten.

- **Co-Managed SOC:**
  Hier arbeiten interne Teams in Zusammenarbeit mit einem externen Dienstleister zusammen. Dieses Modell bietet eine Kombination aus interner Kontrolle und externem Fachwissen.

- **Cloud-basiertes SOC:**
  Dieses Modell beinhaltet die Verlagerung der SOC-Funktionen in die Cloud. Es kann Flexibilität und Skalierbarkeit bieten, insbesondere für Organisationen mit dezentralen Standorten.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontaktsuresecure.de
www.suresecure.de